# Une nouvelle étude révèle la vulnérabilité des e-commerçants français face au piratage de compte

Près de 40% des e-commerçants ont déclaré qu'au moins un compte client sur dix a été victime de piratage l'année dernière en France. C'est ce que révèle une enquête menée par Riskified, fournisseur de solutions de paiement et de prévention de fraude, auprès de 100 commerçants et 1 000 consommateurs français. Ces attaques (dites *Account Takeover* ou ATO) surviennent lorsqu'un fraudeur prend le contrôle d'un compte en se servant des identifiants du titulaire légitime et l'utilise à des fins malveillantes.

Cette étude démontre à quel point cette forme de fraude a des répercussions négatives pour les enseignes, portant préjudice à la fois à leur réputation et à leur chiffre d'affaires. Malgré cela, 24% des professionnels interrogés admettent n'avoir aucune solution pour se prémunir contre le piratage, par crainte sans doute de compromettre l'expérience d'achat. Pourtant, 52% d'entre eux pensent que la crise du COVID-19 va inévitablement conduire à une augmentation de la fraude e-commerce.

63% des e-commerçants et 90% des acheteurs craignent que leurs comptes ne soient piratés. Les ATO peuvent coûter particulièrement cher aux sites marchands : 76% des utilisateurs interrogés déclarent qu'ils cesseraient d'effectuer des achats en ligne auprès du site où leur compte a été piraté et plus d'un tiers iraient chez un concurrent.

Malheureusement, les e-commerçants semblent démunis pour parer à ce type d'attaque : 18% des détaillants interrogés déclarent ne pas avoir la capacité de détecter une usurpation de compte durant le processus d'achat et 10% déclarent ignorer qu'un piratage a eu lieu à moins que la victime ne les contacte.

Les mesures adoptées par ceux qui tentent de se protéger augmente la friction et nuisent à l'expérience client. 40% des professionnels interrogés indiquent appliquer une authentification forte pour certaines tentatives de connexion et 68% exigent des mots de passe complexes. Cependant, la moitié des clients reconnaissent utiliser le même mot de passe pour plusieurs de leurs comptes en ligne.

« *Notre enquête montre que les marchands sont préoccupés par les attaques ATO, mais ils ne sont généralement ni en mesure de les identifier, ni de les éviter* » selon Assaf Feldman, cofondateur et directeur technique de Riskified. « *Sans une analyse dynamique et exhaustives de toutes les données pertinentes, les e-commerçants s'exposent à des pertes financières, des clients mécontents et une réputation ternie. Des solutions s'appuyant sur le machine learning permettent d'identifier les clients légitimes en temps réel, facilitant leur progression dans le tunnel d'achat. Les comportements suspects sont immédiatement vérifiés et bloqués, prévenant efficacement ce genre d'attaque. De ce fait, les détaillants augmentent leurs ventes, tout en offrant à leurs clients une expérience de qualité* ».

En raison des effets délétères des attaques AT0 et de la difficulté à les détecter, les e-commerçants

doivent s'appuyer sur le plus de données possibles pour pouvoir se protéger efficacement. Par exemple, prendre en compte l'appareil, le réseau utilisé, l'éventuelle utilisation d'un proxy et analyser les connexions antérieures pour déterminer s'il s'agit bien du titulaire du compte. Si l'un de ces éléments est inhabituel ou présente les signes caractéristiques d'un piratage, il est préférable de se mettre directement en relation avec le propriétaire légitime, voire d'imposer une authentification forte.

La prise de contrôle d'un compte n'est pas l'objectif final d'un fraudeur, ce qu'il veut, c'est passer des commandes. Ceci permet aux sites marchands d'examiner leurs actions: une connexion inhabituelle ou une modification des coordonnées peut sembler suspecte au départ, mais si le panier est à faible risque au moment du paiement, la commande peut être approuvée en toute sécurité. Lorsque des actions à priori légitimes sont suivies par un impayé frauduleux, les détaillants doivent scrupuleusement examiner les activités du compte et encourager le client à modifier son mot de passe. Cette surveillance tout au long du parcours d'achat permet de réduire les risques et d'augmenter la conversion.

Autres conclusions :

Les comptes fidélité sont une option d'achat très utilisée par les clients :

- 87% de ces derniers déclarent posséder un compte de ce type pour effectuer leurs achats
- 52 % effectuent la plupart de leurs achats auprès de sites où ils ont ouvert un compte
- 60% déclarent acheter plus fréquemment lorsqu'ils détiennent un compte

Les clients détenteurs d'un compte sont intéressants pour les commerçants :

- Plus des deux tiers (69%) des détaillants interrogés déclarent qu'au moins la moitié de leurs commandes proviennent d'acheteurs ayant un compte
- Près de la moitié d'entre eux (47.5%) indiquent que les titulaires de compte dépensent plus par achat que les autres
- 49% estiment que la création de compte incite les clients à acheter plus souvent

Des statistiques supplémentaires issues de cette enquête seront présentées lors d'un webinaire qui aura lieu le 16 juin à 17h, heure de Paris. Plus d'informations à ce sujet sont disponibles ici : https://pages.riskified.com/ato-survey-webinar/

## Méthodologie

Les enquêtes ont été réalisées par Propeller Insights pour le compte de Riskified, avec des questions à réponses multiples adressées à un échantillon de 1000 consommateurs français qui ont pour habitude de faire du shopping en ligne et à 100 professionnels du e-commerce, en France. Les professionnels interrogés occupent l'une des fonctions suivantes : Directeur sécurité des systèmes d'information, Directeur informatique, Directeur CRM et fidélisation, Directeur des paiements, Directeur/ responsable financier, Responsable revenue assurance, Directeur e-commerce/ digital/ omnicanal, Directeur/ responsable fraude.

## À propos de Riskified :

Expert dans l'utilisation de l'IA, Riskified permet au sites marchands d'atteindre leur potentiel de

croissance en toute sécurité. Compagnies aériennes, marques de luxe et bien d'autres : les plus grandes enseignes nous font confiance pour augmenter leur rentabilité, gérer leur risque et améliorer l'expérience client. Les commerçants perdent des milliards à cause de mesures de sécurité trop restrictives, imposées par des solutions antifraudes obsolètes ou inadaptées. S'appuyant sur ses algorithmes le machine learning, Riskified parvient à identifier les acheteurs légitimes instantanément et à maximiser les taux de conversion. Les commerçants peuvent valider un plus grand nombre de commandes, s'étendre à l'international et éliminer toute friction de leurs flux omnicanaux. www.riskified.com